Een strafvorderlijke gegevensvergaring nieuwe stijl

Stevens, L.; Koops, E.J.; Wiemans, F.P.E.

Published in:
Nederlands Juristenblad

Publication date:
2004

L. Stevens, B.J. Koops & P. Wiemans (2004), 'Een strafvorderlijke gegevensvergaring nieuwe stijl'
Verschenen in: Nederlands Juristenblad 79 (32), p. 1680-1686.

Strafvorderlijke gegevensvergaring nieuwe stijl

Lonneke Stevens, Bert-Jaap Koops & Paul Wiemans[1]

Inleiding

'Een muisstille revolutie in het strafrecht', 'De stilzwijgend uitdijende opsporingsvergaarbak',[2] het zijn zo wat benamingen voor het nieuwe arsenaal aan strafvorderlijke bevoegdheden tot gegevensvergaring. Met verbazingwekkend weinig tamtam werd in februari 2004 een algemeen wetsvoorstel vorderen gegevens ingediend, nadat *en passant* al twee sectorale wetten waren ingevoerd. De drie regelingen hangen samen met het rapport van de Commissie-Mevis waarin algemene nieuwe uitgangspunten voor gegevensvergaring in strafvordering werden geformuleerd. Het wetsvoorstel vorderen gegevens voert die uitgangspunten door voor de 'algemene' strafvordering.[3]

De nieuwe bevoegdheden moeten worden bezien tegen de achtergrond van de informatiemaatschappij, waarin gegevens steeds meer zelfstandige waarde krijgen. Dat betreft niet alleen gegevens met geldswaarde, zoals adressenbestanden, maar vooral ook gegevens met informatiewaarde. Voor de opsporing lonkt een mekka van bestanden, registraties en computersystemen, waarin over elke verdachte, elk slachtoffer, hun hele familie-, vrienden- en kennissenkring, ja zelfs over hun losse contacten met vreemden en bedrijven, en ook over hun auto's, mobieltjes en bankrekeningen, wel iets te vinden valt. Daarbij kunnen verbanden worden gelegd en kan inzicht worden verkregen in geld- en goederenstromen, in het vermogen, het relatienetwerk of de handel in bepaalde goederen. De huidige bevoegdheden om al dergelijke gegevens op te vragen, schieten te kort, en medewerking op vrijwillige basis zorgt voor problemen.[4]

Het is in dat licht goed dat nieuwe bevoegdheden zijn voorgesteld. Maar het mag niet zo zijn dat de wet wordt aangepast zonder aandacht voor de belangen van burgers en bedrijven die de gegevens moeten verstrekken en van de mensen op wie de gegevens betrekking hebben: u en wij. Het door de wetgever benadrukte 'belang van de opsporing' verdient een weerwoord. Wij vatten daartoe in deze bijdrage, na een schets van de voorstellen, de in de literatuur genoemde kritiek samen en geven onze visie op deze 'revolutie in het strafrecht'.

1. De bevoegdheden tot het vorderen van gegevens

In de huidige regeling kunnen opgeslagen gegevens alleen worden opgevraagd door de rechter-commissaris tijdens een gerechtelijk vooronderzoek (art. 125i Sv). Dat is inmiddels hopeloos verouderd: het gvo is bij de wet Herziening gerechtelijk

[1] De auteurs zijn werkzaam bij de Universiteit van Tilburg, Lonneke Stevens als promovenda bij de vakgroep Strafrechtswetenschappen, Bert-Jaap Koops als uhd recht & techniek bij TILT, Centrum voor Recht, Techniek en Samenleving, en Paul Wiemans als universitair docent bij de vakgroep Strafrechtswetenschappen. Een uitgebreidere versie van dit artikel is te vinden op <http://www.gegeven.nl>.

[2] Zie Asscher & Koops, 'Een muisstille revolutie in het strafrecht', *Het Financieele Dagblad*, 1 april 2004 en J.E.J. Prins, 'De stilzwijgend uitdijende opsoringsvergaarbak', *NJB* 2004, p. 823.

[3] Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij, *Gegevensvergaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*, mei 2001, hierna: Rapport Commissie-Mevis 2001, te vinden op <http://www.gegeven.nl> onder 'Documenten'. De paginanummers waar hierna naar verwezen wordt, refereren aan deze elektronische versie van het rapport. De wetsvoorstellen (algemeen: 29 441; financiële sector: 28 353, Stb. 2004, 109; telecommunicatie: 28 059, Stb. 2004, 105) en de reacties op het rapport en de wetsvoorstellen zijn te vinden op <http://www.gegeven.nl>.

[4] Commissie-Mevis 2001, p. 25 e.v, *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 1-2, 17.

vooronderzoek (Stb. 1999, 243) uitgekleed en losgekoppeld van de uitoefening van ingrijpende bevoegdheden, en bovendien is het inzetten van de r-c bij relatief simpele gegevens nogal disproportioneel. In de praktijk wordt dan ook vaak het bevel tot uitlevering van voorwerpen gebruikt (namelijk van een gegevensdrager), art. 96a of 105 Sv, of er wordt om vrijwillige medewerking van de gegevenshouder verzocht. In het laatste geval moet de houder zelfstandig een afweging maken tussen het opsporingsbelang en het privacybelang van de betrokkene (art. 8 onder e j^{o} art. 43 Wet bescherming persoonsgegevens). Beide situaties zijn – voorzichtig uitgedrukt – niet ideaal.[5]

Het nieuwe arsenaal aan bevoegdheden is aanzienlijk uitgebreider en meer gevarieerd. Het wetsvoorstel beslaat drie hoofdbevoegdheden, voor identificerende, algemene en gevoelige gegevens. Deze vervangen artikel 125i, dat vervalt.[6]

Allereerst kan de opsporingsambtenaar op grond van de artikelen 126nc en 126uc Sv identificerende gegevens opvragen, en wel bij verdenking van een misdrijf of in geval van artikel 126o lid 1 Sv.[7] Het gaat hier om naam, adres, woonplaats, geboortedatum en geslacht, en administratieve kenmerken, zoals het nummer van de airmiles-pas, het lidnummer van de sportvereniging, en bankrekeningnummers. De vordering wordt gericht tot personen die dergelijke gegevens verwerken, anders dan voor persoonlijk gebruik. In de praktijk kan de politie hiermee eenvoudig nagaan bij een bank, een postorderbedrijf, een videotheek, een supermarkt of een sport- of culturele vereniging of iemand daar een klant of lid is. De politieagent kan zo bijvoorbeeld verbanden leggen tussen personen, bijvoorbeeld om te kijken wie zoal contact kan hebben met een verdachte fraudeur binnen de golfclub.[8]

In de tweede plaats krijgt de officier van justitie de bevoegdheid om 'andere dan identificerende' gegevens op te vragen (artikelen 126nd en 126ud Sv). Dan gaat het om informatie over een dienst die geleverd is, bijvoorbeeld het soort videobanden dat geleend is, welke boeken iemand hoe lang heeft geleend bij de bibliotheek, of hoeveel boodschappen iemand de afgelopen maand heeft afgerekend met zijn klantenpas, en ook – als de supermarkt dat bijhoudt – welke boodschappen dat precies waren.[9] Het kan dus om zeer privacygevoelige gegevens gaan, en daarom mag de bevoegdheid alleen worden ingezet bij zwaardere misdrijven, namelijk die worden genoemd in artikel 67, eerste lid Sv, grofweg misdrijven met een maximum van vier jaar gevangenisstraf of hoger. Het hoeft echter niet om verdachten te gaan: de officier mag over iedereen gegevens opvragen als hij denkt dat dit nuttig is voor een opsporingsonderzoek. De vordering van deze gegevens kan zelfs betrekking hebben op toekomstige gegevens (artikelen 126ne en 126ue Sv). Dat zijn gegevens die pas na het tijdstip van de vordering worden ontvangen, opgeslagen, vastgelegd, of op een

[5] Zie nader over art. 125i en de beperkingen op basis van het huidige recht: F.P.E. Wiemans, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: WLP 2004, p. 125 e.v.

[6] Het wetsvoorstel vervangt art. 125i door een geheel nieuw art. 125i, dat de doorzoeking ter vastlegging van gegevens regelt. Een dergelijke doorzoeking vond voorheen plaats op grond van de bevoegdheid tot doorzoeking met het oog op inbeslagneming – waarop in feite de doorzoeking dus niet was gericht, aangezien gegevens als zodanig niet in beslag genomen kunnen worden (zie daarover Wiemans 2004, a.w., p. 234-238). Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 11.

[7] De gevallen van artikel 126o lid 1 Sv hebben betrekking op het ruimere verdenkingscriterium in verband met de georganiseerde misdaad: 'Indien uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven als omschreven in artikel 67, eerste lid worden beraamd op gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren (…)'.

[8] De beschrijving van de bevoegdheden en de voorbeelden is mede gebaseerd op Asscher & Koops 2004, a.w.

[9] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 8.

andere manier verwerkt.[10] Het gaat dan bijvoorbeeld om video's die iemand in de komende vier weken huurt of boodschappen die hij de komende weken zal doen. De officier kan zelfs, met machtiging van de rechter-commissaris, bevelen dat het bedrijf deze gegevens steeds direct doorstuurt aan justitie.
Met machtiging van de rechter-commissaris kunnen ten derde ook gevoelige gegevens worden opgevraagd, bij zware misdrijven die een ernstige inbreuk op de rechtsorde maken (artikel 126nf), of indien het belang van het onderzoek dit dringend vordert (126uf). Gevoelige gegevens zijn gegevens over iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging. Dit stelt beperkingen aan de gegevens die de officier van justitie kan opvragen: boeken of video's over ziektes, seks of godsdienst en boodschappen van suikervrije producten zijn gevoelige gegevens. Daarom zou de officier niet zomaar bij elke videotheek, bibliotheek of supermarkt alle gegevens mogen opvragen. Het probleem is alleen dat de gevoeligheid van gegevens niet vooraf kenbaar zal zijn. Daarom kan de officier vermoedelijk gewoon alle gegevens opvragen, en eventuele gevoelige video's of boodschappen als 'bijvangst' tellen.

Voor al deze bevoegdheden geldt dat meewerking verplicht is: het weigeren gegevens te verstrekken is strafbaar op grond van artikel 184 Sr. Strafbaarheid zal overigens wel afhangen van de waarschijnlijkheid dat de houder de gegevens ook echt heeft. Die hoeft niet groot te zijn: opvragen is al mogelijk als 'de opsporingsambtenaar *aanwijzingen* heeft, *hoe licht ook*, die erop *wijzen* dat er een *kans* is dat deze gegevens heeft van de persoon die onderwerp is van onderzoek' [onze cursivering].[11]
Overigens mogen de vorderingen niet aan de verdachte worden gegeven, en ook voor verschoningsgerechtigden zijn uitzonderingsbepalingen voorzien.

Nevenbevoegdheden

Naast de hoofdbevoegdheden zijn nog enkele nevenbevoegdheden relevant. Dat is in de eerste plaats de mogelijkheid om *ontsleuteling* van gegevens te vorderen (artikelen 126nh en 126uh Sv), als onverhoopt de overhandigde gegevens vercijferd blijken te zijn. Dit ontsleutelbevel kan volgens de tweede leden niet aan de verdachte worden gegeven. De bevoegdheid is vergelijkbaar met het huidige artikel 125k Sv, dat ontsleuteling tijdens een doorzoeking regelt. Merkwaardigerwijs vervalt echter bij dat artikel juist de uitzondering voor verdachten en verschoningsgerechtigden, door een redactionele aanpassing van art. 125m Sv.[12] Daardoor schept het wetsvoorstel feitelijk

[10] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 24-25.

[11] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 20. Zie ook Mac Gillavry 2004, p. 546. De Commissie-Mevis loste dit probleem op door middel van het stellen van ja/nee-vragen ('is deze persoon klant bij u?' 'Houdt u een dagboek bij?'). In het kabinetsstandpunt werd deze benadering echter afgewezen. De bevoegdheid tot het stellen van voorvragen werd ingelezen in de bevoegdheid tot vorderen van gegevens zelf, hetgeen materieel op hetzelfde neerkomt. *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 14.

De lage zekerheidsgraad levert nog een ander potentieel probleem op, vanwege de grenzen die het Europees Hof lijkt te stellen aan het onder sanctiebedreiging vorderen van documenten. Een gangbare interpretatie van de arresten *Funke* en *J.B.* is immers dat de vorderingen in die gevallen niet door de beugel konden omdat de autoriteiten niet zeker wisten of de gevraagde stukken wel bestonden. Het uitleveren van gegevens kan in dergelijke situaties een verklarende waarde hebben ('ja, ik ben mij bewust van de gegevens'), waardoor strijd met het nemo-teneturbeginsel kan ontstaat als de gegevens vervolgens als strafrechtelijk bewijs tegen de gegevenshouder worden gebruikt. Zie B.J. Koops & L. Stevens, 'J.B. versus Saunders: de groeiende duisternis rond nemo tenetur', *Delikt & Delinkwent* maart 2003, p. 281-294.

[12] In de nieuwe redactie van artikel 125m keren de huidige leden 1 en 2 niet terug. Het lijkt erop dat de regering zich heeft blindgestaard op art. 125i; nu dat komt te vervallen en de bescherming van verdachten en verschoningsgerechtigden wordt overgeheveld naar elke afzonderlijke nieuwe bevoegdheid (art. 126nc lid 3, 126nd lid 2, enz.), heeft de regering kennelijk

de mogelijkheid om verdachten en verschoningsgerechtigden te dwingen te ontsleutelen tijdens een doorzoeking. Aangezien dit nergens wordt toegelicht of gemotiveerd, en de bescherming voor verdachten en verschoningsgerechtigden wel wordt ingevoerd bij de nieuwe bevoegdheden, gaan wij ervan uit dat de wetgever deze wijziging niet daadwerkelijk heeft beoogd. Het wetsvoorstel moet op dit punt dan ook worden aangepast.

Een tweede nevenbevoegdheid is *bevriezing* van gegevens. Dit is relevant als justitie gegevens wil vorderen die vluchtig zijn en die de houders ervan misschien niet zo lang bewaren dat de justitie ze zou kunnen opvragen. Dit komt bijvoorbeeld voor bij op het Internet gesignaleerde kinderpornografie die de houder ervan niet, of slechts kort, bewaart,[13] of als gegevens uit het buitenland nodig zijn.[14] De door de Commissie-Mevis voorgestelde bevriezingsbevoegdheid is niet opgenomen in het wetsvoorstel vorderen gegevens, maar in het ontwerpvoorstel Aanpassing aan het Cybercrime Verdrag.[15] Art. 126ni Sv biedt de hulpofficier de bevoegdheid om bij een misdrijf als omschreven in artikel 67, eerste lid Sv te vorderen dat gegevens gedurende ten hoogste 90 dagen beschikbaar worden gehouden. Dit is een ruimere bevoegdheid dan de Commissie-Mevis voorstelde: die eiste dat het misdrijf een ernstige inbreuk op de rechtsorde opleverde en dat het onderzoek het bevel dringend vorderde; bovendien vond de commissie een bevriezingstermijn van twee weken voldoende in de Nederlandse context.[16] Het huidige voorstel van de minister is aanzienlijk soepeler: naast een lange bevriestermijn wordt een lagere autoriteit – de hulpofficier – bevoegd verklaard, en de eisen van ernstige inbreuk en dringendheid die in een eerder kabinetsstandpunt werden gehanteerd, vervallen.[17]

Een laatste nevenbevoegdheid is de mogelijkheid om *bewerken* van gegevens te vorderen, waardoor nieuwe gegevens ontstaan (door de Commissie-Mevis voorgesteld in een nieuw artikel 126ng Sv). Door *datamining* of registervergelijking zou men bijvoorbeeld kunnen achterhalen wie van degenen die op 12 maart 2004 geld hebben opgenomen bij een flappentap in Amsterdam, in de week daarna van Schiphol zijn weggevlogen of een auto hebben gehuurd, of wie van degenen die in april een messenset bij een Blokker kochten, op 14 mei in Deventer mobiel gebeld hebben. Dergelijke bewerking vormt een belangrijke bron van informatie voor strafvorderlijk onderzoek en moet dus mogelijk worden gemaakt. De Commissie-Mevis verbond wel 'zware' voorwaarden aan deze bepaling.[18] Anders dan de Commissie, kiest het

gedacht dat art. 125m leden 1-2 niet meer nodig zijn. Daarmee miskent zij echter dat deze bepalingen ook relevant zijn voor het algemene beveiligingsdoorbrekingsbevel van art. 125k, dat gewoon blijft bestaan.

[13] Commissie-Mevis, p. 70.

[14] In het Cybercrime-verdrag (Boedapest 23 november 2001, *Trb.* 2002, 18; zie *Computerrecht* 2003 nr. 2) is een steunmaatregel opgenomen om de veiligstelling of bevriezing ('preservation') van gegevens te bevelen. De in Nederland voorgestelde bevriezingsbevoegdheid is mede hierop gebaseerd.

[15] Zie <http://www.justitie.nl>, klik achtereenvolgens 'thema', 'wetgeving", 'wetgeving in voorbereiding', 'straf- en sanctierecht'.

[16] Commissie-Mevis 2001, p. 71.

[17] Zie over de termijn *Kamerstukken II* 2001/01, 28 366, nr. 1, p. 22, en Buruma & Koops, 'Formeel strafrecht en ICT', in Koops (red.), *Strafrecht en ICT*, Sdu 2004, p. 97. De eis van dringendheid werd bij de Commissie-Mevis ingegeven door de doelafwijkende verwerking van de te bevriezen gegevens waar het bevel toe noodzaakt. De eis van ernstige inbreuk op de rechtsorde nam het kabinet nam aanvankelijk over vanwege gewenste terughoudendheid door de lasten voor het bedrijfsleven en de bijzondere inspanning die veelal zal worden gevraagd. Het kabinet wilde oorspronkelijk ook de bevoegdheid voorbehouden aan de officier van justitie en niet aan de hulpofficier, mede vanwege de langere bevriezingstermijn. Zie *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 22.

[18] Commissie-Mevis, p. 67. De bevoegdheid ligt bij de officier van justitie indien het belang van het onderzoek dit dringend vordert, na machtiging van de r-c, in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid Sv, dat gezien zijn aard of samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde

kabinet er echter voor om niet bedrijven en burgers, maar de politie dergelijke bewerkingen te laten uitvoeren,[19] wellicht mede vanwege kritiek dat houders van gegevens anders te actief betrokken zouden worden bij de opsporing.[20] In het wetsvoorstel vorderen gegevens is echter niets over bewerking terug te vinden. Vermoedelijk wordt bewerken nu opgevat als een logisch uitvloeisel van de bevoegdheden tot het vorderen van gegevens, en behoeft het geen zelfstandige regeling. Het gevaar hiervan is dat soms meer gegevens zullen worden opgevraagd dan wanneer het ('bij')doel van bewerken er niet was.[21] Wij zien daarom liever een wettelijke regeling die eisen stelt aan de gevallen waarin en de gronden waarop bewerking zou mogen worden toegepast.

De sectorale wetten

In het Staatsblad zijn begin 2004 aanpalende wetten verschenen, voor gegevens in de financiële sector en in de telecommunicatiesector.[22] De eerste wet betreft bevoegdheden die identiek zijn aan de bevoegdheden in het hierboven besproken wetsvoorstel gegevensvergaring, met dit verschil dat uitsluitend gegevens worden gevorderd van 'een ieder die beroeps- of bedrijfsmatig een financiële dienst verleent'. Deze wet werd nodig geacht om versneld een EU-protocol in het kader van terrorismebestrijding in te kunnen voeren. Deze regeling zal echter vervangen worden door de algemene regeling tot het vorderen van gegevens.[23]
De verhouding tussen de wet voor de telecommunicatiesector en de algemene gegevensvergaring ligt iets ingewikkelder. Voor telecommunicatie bestaat al sinds 1926 een regime (zie de huidige artikelen 126n, 126na, 126u en 126nu Sv), en volgens de wetgever is hier sprake van een gegroeide praktijk met speciale behoeften, zoals het direct doorgeleiden aan justitie van gegevens wie wanneer met wie belt.[24] Deze categorieën gegevens (gebruikersgegevens en verkeersgegevens) worden uitgesloten in het algemene wetsvoorstel gegevensvergaring; het gaat dus om aanvullende bevoegdheden.[25] Dit lijkt ons een zwaktebod: juist wanneer men een integrale visie ontwikkelt op gegevensvergaring in de huidige maatschappij, moet men geïntegreerd kijken naar alle mogelijke soorten gegevens en moet men ook historisch gegroeide praktijken onder de loep willen nemen.

oplevert, dan wel in geval van het verdenkingscriterium van 126o Sv.

[19] Het bewerken dient door opsporingsambtenaren te worden uitgevoerd, op bevel van de officier, na machtiging van de r-c. *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 20.

[20] Zie bijvoorbeeld het advies van het CBP, <http://www.gegeven.nl>, onder reacties.

[21] De Commissie-Mevis wijst ook op deze mogelijkheid. Commissie-Mevis, p. 68.

[22] Wet vorderen gegevens financiële sector, *Stb.* 2004, 109, en Wet vorderen gegevens telecommunicatie, *Stb*. 2004, 105.

[23] Protocol bij de Overeenkomst betreffende wederzijdse rechtshulp in strafzaken tussen de Lid-Staten van de EU. Zie verder *Kamerstukken II* 2001/02, 28 353, nr. 3, p. 3 en *Kamerstukken II* 2002/03, 28 353, nr. 6, p. 1-2.

[24] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 14. Zie ook het kabinetsstandpunt, *Kamerstukken II* 2001/02, 28 366, nr. 1, p. 29-30 en de Commissie-Mevis, p. 90-92.

[25] De algemene bevoegdheden uit het wetsvoorstel zullen alleen kunnen worden toegepast bij telecomaanbieders als de vordering betrekking heeft op ándere dan verkeers- en gebruikersgegevens, aldus artikelen 126ng en 126ug Sv van het wetsvoorstel vorderen gegevens. Het gaat dan bijvoorbeeld om de inhoud van opgeslagen telecommunicatie, zoals een opgeslagen e-mailbericht of een stempostbericht die ligt opgeslagen bij de aanbieder. Zie nader *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 14.

2. Kritiekpunten

2.1. Inbreuk op privacy

In 2002 kwam de Commissie-Mevis al de twijfelachtige eer toe een Big Brother Award in ontvangst te mogen nemen voor 'het slechtste plan voor de privacy'.[26] En ook vanuit andere hoek is veel kritiek geleverd op het op grote schaal mogelijk maken van gegevensvergaring en de daaraan verbonden gevolgen voor de persoonlijke levenssfeer. Zie hier een selectie van kritiek en uitgesproken angsten.

> 'Het meest fundamentele bezwaar dat ik er tegen heb is dat het ons denken over de rechtsstaat corrumpeert. De redenering lijkt te zijn dat ICT het steeds beter mogelijk maakt om de gedragingen van individuen te registreren en te volgen en dat dus de overheid het recht heeft om van deze technische vooruitgang te profiteren door individuele vrijheden verdergaand te beperken'.[27]

> 'Ieder lid van een sport- of hobbyclub of eenieder die deelneemt aan een georganiseerde culturele activiteit is zijn of haar privacy kwijt.'[28]

> 'Maar het gaat wel om een zwaar middel dat de bestaande opsporingsbevoegdheden sterk uitbreidt. En waarmee een grote inbreuk op de privacy kan worden gemaakt, ook van niet-verdachte burgers'.[29]

> 'Alhoewel opsporingsbevoegdheden ook nu worden ingezet tegen niet-verdachte personen (…), is bij de nieuwe vergaringsbevoegdheden sprake van een duidelijke schaalverschuiving: veel meer dan vroeger kunnen gegevens over niet-verdachte personen worden opgevraagd, waardoor de justitiële arm breder doordringt in de maatschappij'.[30]

Uit de citaten komt al naar voren dat de kritiek voornamelijk voortkomt uit de grootschaligheid van de bevoegdheden. Die grootschaligheid ligt ten eerste in het feit dat uiteindelijk elk geregistreerd gegeven waar om wordt gevraagd aan justitie moeten moet worden verstrekt. En elk gegeven wordt wel ergens geregistreerd. Zo kan justitie vragen aan een boekhandel om op te slaan en door te geven welke boeken meneer Jansen koopt met een bepaalde airmilespas of bankpas, of wie *Lolita* heeft gekocht; aan een bank wie geld doneert aan de Stichting Al-Aqsa of Stichting de Regenboog (opvang voor harddruggebruikers); wie op Google gezocht heeft naar zowel "Balkenende" als "tweedehands pistolen"; of aan u wat u het afgelopen jaar in uw dagboek heeft geschreven over uw buurman die de gordijnen altijd dichthoudt.
Dit is des te ingrijpender, nu justitie ook gegevens kan opvragen over niet-verdachte burgers. Zo kan een grofmazig net worden uitgegooid om te kijken met wie een bepaalde verdachte zoal op welke manieren contact heeft gehad, maar ook wie rond het tijdstip van de moord in een straal van tien kilometer mobiel belde, geld opnam of ergens in de buurt met pinpas betaalde. De verkregen resultaten kunnen vervolgens worden verkleind door combinatie en reductie. Vanwege de grootschaligheid van opgeslagen computergegevens, komen burgers hierdoor sneller dan voorheen in het vizier van justitie. Zoals Mac Gillavry signaleert lijkt de politiek uit te gaan van het

[26] Zie <http://www.netkwesties.nl/editie31/artikel2.html>.
[27] E. Dommering, 'Het ongebreideld verzamelen van gegevens: de voorstellen van de Commissie Mevis', beschikbaar op <http://www.gegeven.nl> onder 'reacties'.
[28] F. Kuitenbrouwer, 'Moderne inquisitie', <http://www.gegeven.nl>, beschikbaar op onder 'reacties'.
[29] Asscher & Koops 2004, a.w.
[30] J.E.J. Prins, 'De stilzwijgend uitdijende opsoringsvergaarbak', *NJB* 2004, p. 823.

motto 'wie niets te verbergen heeft, heeft niets te verliezen'. Hij stelt echter terecht dat niet-verdachte burgers wel degelijk wat te vrezen hebben van een onderzoek, namelijk hun goede naam als betrouwbaar burger waarmee bedrijven veilig zaken kunnen doen. Een bank zal de volgende keer misschien geen lening verstrekken als de politie navraag heeft gedaan.[31] En wanneer de politie de boekhandel in het dorp vraagt of meneer Jansen ooit boeken over seks, naaktfotografie of pedofilie heeft gekocht, zal de boekhandelaar de volgende keer toch met andere ogen naar Jansen kijken. Waar critici aldus een aanzienlijke verschuiving zien naar instrumentaliteit ten koste van privacy, lijkt de politiek met heel andere zaken bezig. Tekenend is de opmerking van de CDA-fractie:

> 'Deze leden [CDA] vragen of het denkbaar zou zijn geweest om dit voorstel meer te bezien vanuit de opsporingskant, waarbij eventuele strijdigheid met de Wet bescherming persoonsgegevens tot wijziging van die wet zou moeten leiden'.[32]

Niet de persoonlijke levenssfeer maar het belang van de opsporing, en uiteraard het belang van terrorismebestrijding, worden meermalen benadrukt. In deze tijden van onveiligheidsgevoelens lijkt beroep op aandacht voor privacy kansloos. Toch verdient het aanbeveling dat de Kamer haar perspectief wat verlegt. Het wetsvoorstel zelf legt immers toch al veel gewicht in de schaal bij de opsporing, meer nog dan de Commissie-Mevis zelf. Als de privacy niet volledig uitgekleed moet worden in de nabije toekomst, dan zal het parlement – gegeven het huidige politieke klimaat in de regering – het op zich moeten nemen om ook naar privacybelangen te kijken. De balans kan alleen worden gevonden wanneer er evenwichtige aandacht is voor alle in het geding zijnde belangen.

2.2. Rechtsbescherming

De kritiek op de inbreuk op de persoonlijke levenssfeer staat grotendeels ook in verband met de waarborgen waarmee de nieuw gecreëerde bevoegdheden zijn omkleed. Deze zouden een onvoldoende niveau van rechtsbescherming aan de burger bieden.

Het systeem dat de Commissie-Mevis voor ogen had opdat de bevoegdheden met inachtneming van de belangen van de objecten-van-onderzoek worden toegepast, is overgenomen in het wetsvoorstel. Uitgangspunt is het getrapte stelsel waarbij naarmate de gegevens gevoeliger worden, de autoriteit die gegevens vordert hoger is en het verdenkingscriterium zwaarder. Verdere waarborgen zijn de notificatieplicht (artikel 126bb Sv wordt daartoe aangepast), waarbij de betrokken burger op de hoogte wordt gesteld van het onderzoek, en het beklagrecht (een aangepast artikel 552a Sv). Ook de eis dat in vrijwel alle gevallen de vordering schriftelijk moet worden gedaan, wordt gezien als een mechanisme dat zal zorgen voor zorgvuldige toepassing van de bevoegdheden.[33]

Feit blijft echter dat de belangenafweging volledig in handen van justitie is gelegd, waarbij alleen gevoelige gegevens en toekomstige direct door te leiden gegevens zijn onderworpen aan een machtiging van de rechter-commissaris. (Overigens moet wel worden aangetekend dat bedrijven, blijkens het onderzoek van

[31] Mac Gillavry 2004, p. 489.
[32] *Kamerstukken II* 2003/04, 29 441, nr. 5, p. 1.
[33] Zie rapport-Mevis, p. 73-74.

Mac Gillavry, ook niet bepaald enthousiast de belangen van de 'onderzoeksobjecten' behartigen in geval van vrijwillige samenwerking.[34]) Het is nog maar de vraag of de natuurlijke informatiehonger van politie en justitie voldoende wordt 'tegengewerkt' door bovengenoemde vereisten van schriftelijkheid, verbaliseringsplicht en notificatie. Naar oordeel van het CBP leert de ervaring dat het slechts papieren garanties zijn. Het CBP ziet dan ook meer heil in het verplicht vergoeden van de kosten door de overheid. Vergoeding voor elke bevraging zou wél de nodige terughoudendheid kunnen realiseren en zo een economische rechtswaarborg vormen.[35]

Commissievoorzitter Mevis erkent ook het gevaar dat de politie binnen de gegeven bandbreedte wellicht niet altijd even terughoudend zal opereren (en overigens ook het gevaar dat de politie buiten die bandbreedte treedt). Hij ziet de verzekering voor zorgvuldigheid in het gebruik van de bevoegdheden met name liggen in de afspraken die op uitvoeringsniveau worden gemaakt met bedrijven en binnen sectoren.[36] We moeten echter afwachten hoe dergelijke afspraken tot stand zullen komen, om te weten of bedrijven en sectoren echt tegenwicht kunnen en willen bieden tegen de informatiehonger van justitie.

Belangrijk is in elk geval dat de toepassing van de bevoegdheden ook altijd achteraf kan worden gecontroleerd. De Memorie van Toelichting van het wetsvoorstel meent dat de eisen van verbalisering en verslaglegging tegemoet komen aan deze eis.[37] Ook wordt de aanbeveling van het CBP gevolgd om in de Wet politieregisters een verplichting op te nemen tot het houden van een *audit* op de gegevensverwerking door de politie.[38] Enige skepsis is echter gepast over de mate waarin verbalisering en verslaglegging daadwerkelijk tot controleerbaarheid zullen leiden. Naar verwachting zal de bevoegdheid, zeker bij identificerende gegevens, in zeer grote aantallen worden toegepast, en er bestaat een wezenlijk risico dat verbalisering en verslaglegging eerder papier-tijger-routinewerk zullen zijn dan een tijger met tanden die afschrikt tegen overmatige toepassing. Bovendien vindt uitoefening van de bevoegdheden grotendeels in het voortraject van de opsporing plaats; het is daarom sterk de vraag of de uitoefening van de bevoegdheden in veel gevallen bij de zittingsrechter zal belanden die de rechtmatigheid van de uitoefening kan toetsen.

2.3. Kosten en lastenverdeling

Met het kostenaspect van de nieuwe meewerkplichten is de wetgever in het voorstel vorderen gegevens vrij snel klaar. Extra personeelskosten en administratiekosten voor bedrijven komen voor vergoeding in aanmerking voor zover deze inzichtelijk gemaakt kunnen worden.[39] Dit dient geregeld te worden in een aangepast artikel 592 Sv, dat nu de kostenvergoeding voor de meewerkverplichting van onder andere artikel 125i Sv bepaalt. (Binnen het kader van de bestaande regelgeving bestaan beperkte

[34] E.C. Mac Gillavry, *Met wil en dank. Een rechtsvergelijkend onderzoek naar de medewerking aan strafvordering door bedrijven* (diss. Groningen), Nijmegen: Wolf Legal Publishers 2004, hoofdstuk 4, en p. 468 en 490. Zie ook E.C. Mac Gillavry, *Meewerken aan Strafvordering door banken en internet service providers. Een onderzoek naar wetgeving en praktijk*, Deventer: Gouda Quint 2000.

[35] Zie het advies van het CBP op <http://www.gegeven.nl> onder 'reacties', p. 4.

[36] Zie Mevis in het interview met Netkwesties, oktober 2003, <http://www.netkwesties.nl/editie72/artikel1.php>.

[37] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 5.

[38] Dit maakt onderdeel uit van de herziening van de Wet politieregisters (*Kamerstukken II* 2002/2003, 28 600 IV, nr. 134). Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 15.

[39] *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 17.

vergoedingsregelingen en zijn tussen bedrijven en overheid hier bepaalde afspraken gemaakt. Deze vergoedingen zijn meestal niet kostendekkend.[40])
De kosten van de meewerkverplichtingen zullen echter niet altijd worden vergoed. Zo zal de technologische infrastructuur van bedrijven in bepaalde gevallen moeten worden aangepast om te kunnen voldoen aan bevelen om gegevens direct door te sluizen of te bevriezen. De opslagcapaciteit van computersystemen zal soms substantieel moeten worden uitgebreid als justitie herhaaldelijk 90-daagse bevriezing eist van gegevens die normaliter direct na verwerking worden weggegooid. Deze investerings-, exploitatie- en onderhoudskosten komen, als we de Memorie van Toelichting moeten geloven, niet voor vergoeding in aanmerking. Een precedent kan worden gevonden in de aftapbaarheidsverplichting uit de jaren negentig; daarbij speelden volgens de wetgever 'ook budgettaire overwegingen een rol',[41] oftewel: de overheid kon – of wilde – de kosten voor aanpassing van de infrastructuur niet zelf opbrengen, zodat die voor rekening van het bedrijfsleven kwamen (art. 13.6 Telecommunicatiewet). Waar het daar nog ging om een beperkt aantal telecomaanbieders, die bovendien vergunningplichtig waren, gaat het nu echter om het bedrijfsleven *tout court*, inclusief het MKB. Indien bedrijven daadwerkelijk infrastructurele aanpassingen zullen moeten plegen, kan de overheid die volgens ons niet op het bedrijfsleven zelf afwentelen, niet alleen omdat de kosten voor opsporingsdoeleinden bij de overheid thuishoren, maar ook omdat een dergelijke situatie handelsbelemmerend werkt voor in Nederland gevestigde bedrijven, wat in Brussel de nodige wenkbrauwen zal doen fronsen.

Bij de vergoeding van uitvoeringskosten kan men zich afvragen in hoeverre het mogelijk is het 'extra' van de personele arbeid en de administratie inzichtelijk te maken. Incidentele bevraging zal waarschijnlijk binnen de reguliere bedrijfsvoering worden uitgevoerd door personeel met andere taken. Bij structurele bevraging zullen meer kosten gemaakt worden, zoals algemene bedrijfsvoeringskosten voor extra personeel. Bedrijven kunnen die meerkosten alleen hard maken als zij personeel aanstellen specifiek voor meewerking met justitie, maar dat zal denkelijk alleen bij enkele grootverwerkers als banken en telecombedrijven het geval zijn. En wanneer de uitbreiding van personeelscapaciteit sluipenderwijs plaatsvindt bij geleidelijke toename van justitiële bevraging, is het vermoedelijk moeilijk duidelijk te maken welke personeelsuitbreiding precies geschied is enkel en alleen voor medewerking aan justitie.

Het is dus nog maar de vraag of de verdeling van de lasten in het nieuwe systeem voldoet aan maatstaven van redelijkheid van wat men van bedrijven kan verlangen. Dit is des te klemmender, aangezien het niet alleen om eerlijke lastenverdeling gaat, maar ook om het in toom houden van justitie. Zoals het CBP opmerkte, zijn kosten bij uitstek een reguleringsmiddel om de uitoefening van justitiële bevoegdheden in toom te houden (zie par. 2.2). Ook wat dat betreft valt dus te pleiten voor een daadwerkelijke vergoeding van alle kosten van medewerking aan gegevensvordering, zowel de infrastructurele als de uitvoeringskosten.

[40] Zie bijvoorbeeld Mac Gillavry 2004, p. 176.
[41] *Kamerstukken II* 1994/95, 24 108, nr. 3, p. 1.

2.4. Systeem van het strafrecht

Het grootschalig meewerken aan gegevensvergaring is ook bekritiseerd vanuit strafvorderlijk systematisch oogpunt. Het uitgangspunt van het Wetboek van Strafvordering is dat burgers op vrijwillige basis mogen meewerken aan de strafvordering: zij zijn niet verplicht voor de opsporing interessante informatie te verstrekken.[42] Het vorderen van gegevens zoals voorgesteld zou met deze bestaande systematiek breken. Het zou eveneens betekenen dat het uitgangspunt dat in het opsporingsonderzoek getuigen niet verplicht kunnen worden tot het afleggen van een verklaring, wordt verlaten.[43]

De wetgever en de Commissie-Mevis zien de voorstellen nadrukkelijk niet als een informatieplicht.[44] Gegevens zijn 'iedere weergave van feiten, begrippen of instructies (...) geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken' (art. 80quinquies Sr).[45] Gegevens zijn dus kleurloos, betekenisvrij, en dat maakt ze anders dan informatie, waarbij het wel om de inhoud gaat. Bij informatie gaat het om de subjectieve betekenis die aan gegevens wordt toegekend tegen de achtergrond van persoonlijke kennis, ervaringen en omstandigheden, alsmede de betekenis die gegevens krijgen in combinatie met andere gegevens.

In werkelijkheid gaat het de opsporingsinstanties uiteraard juist wel om de inhoud van de gegevens, om de informatie die uit de gegevens kan worden gehaald.[46] Wanneer politie en justitie gegevens vorderen gebeurt dat vanuit het idee daar informatie uit te destilleren, binnen het kader van een bepaalde verdenking. Dat het ook om informatie gaat blijkt ook uit het niet-consequente gebruik van het kleurloze gegevensbegrip door de wetgever. Het wetsvoorstel vorderen gegevens definieert gegevens als '*informatie* die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm' (ons cursief).[47]

Het leggen van nadruk op gegevens in plaats van het achterliggende doel, informatie, verbloemt de reikwijdte van die bevoegdheden. Juist omdat het gaat om informatie, is er meer aan de hand dan een simpel spiegelbeeld van de uitlevering van voorwerpen. Hoewel die ook tot informatie kunnen leiden, is de informatiewaarde van voorwerpen vaak begrensd. Gegevens hebben echter van nature informatiewaarde, en in de huidige informatiesamenleving bieden gegevens, zeker in combinatie, bijna onbegrensde informatiemogelijkheden. Bovendien ontstaan er gegevens over delen van het menselijk leven die vroeger nooit werden vastgelegd; een voorbeeld daarvan is de locatie van personen, die in toenemende mate – door mobiele telefonie, GPS in de auto, en wellicht ook uniek identificerende RFID-chips in producten – vastgelegd

[42] Zie E.C. Mac Gillavry, 'Gegevensvergaring in de informatiemaatschappij: een strafvorderlijke informatieplicht?. De informatieplicht van de Commissie-Mevis', *RM Themis* 2002, p. 28; E.C. Mac Gillavry, 'De voorstellen van de Commissie-Mevis: dwangmiddelen voor de informatiemaatschappij', *NJB* 2001, p. 1411-1418; G. Knigge, 'De krenten en de pap: Strafvordering 2001, *DD* 2002, p. 228.

[43] Y.G.M. Baaijens-van Geloven & J.B.H.M. Simmelink, 'Normering van de opsporing', in: M.S. Groenhuijsen & G. Knigge, *Dwangmiddelen en rechtsmiddelen. Derde interimrapport onderzoeksproject Strafvordering 2001*, Deventer: Kluwer 2002, p. 479-483.

[44] Zie ook de reactie van Mevis op de kritiek van Mac Gillavry, 'Gegevensvergaring is iets anders dan een informatieplicht', *RM Themis* 2002, p. 3035.

[45] Overigens is deze definitie (en die van geautomatiseerd werk, art. 80sexies Sr) niet in de betekenissentitel van het Wetboek van Strafvordering opgenomen. Zie Wiemans 2004, a.w., p. 238-240, die voorstelt om bedoelde definities wel in laatstgenoemd wetboek op te nemen.

[46] Zie Mac Gillavry 2004, p. 538-552.

[47] Zie *Kamerstukken II* 2003/04, 29 441, nr. 3, p. 7.

kan en zal worden in geautomatiseerde systemen. Om deze redenen is het introduceren van een gegevensplicht niet slechts het vullen van een systematisch tekort in het Wetboek van Strafvordering, dat is ontstaan doordat gegevens niet onder het uitleveringsbevel vallen, maar veel meer dan dat: een substantiële verruiming van de mogelijkheden van justitie om informatie te verzamelen, en daarmee een aanzienlijke verruiming van de mogelijke inbreuk op de persoonlijke levenssfeer van burgers. Dat is een systeemwijziging binnen de strafvordering.

Een tweede aspect van de systematiek van de wet betreft de plaats van het onderzoek van computers en gegevens. Dit is nu gezamenlijk geregeld in art. 125i-125n Sv, waarbij zowel het opvragen van gegevens, de doorzoeking, als algemene aspecten aan de orde zijn. Dit laatste betreft bijvoorbeeld bewaring en vernietiging (art. 125n) en gegevens van geheimhouders (art. 125l).
Het wetsvoorstel hevelt echter het vorderen van gegevens over van deze afdeling naar de bijzondere opsporingsbevoegdheden (titel IVA e.v. Sv), waardoor de BOB-regeling voor notificatie (art. 126bb) en bewaring en vernietiging (art. 126cc-dd) van toepassing wordt.[48] Hierdoor ontstaan moeilijk te verklaren verschillen voor bewaring en vernietiging: bij onderzoek in computers moeten gegevens direct worden vernietigd als ze niet relevant zijn (125n);[49] gevorderde gegevens moeten echter altijd worden bewaard tot tot twee maand na afloop van de zaak (126cc). Ook de notificatieplicht verschilt: bij een doorzoeking hoeven niet-verdachten over wie gegevens zijn vergaard, niet in kennis te worden gesteld (art. 125m wetsvoorstel vorderen gegevens), maar bij gevorderde gegevens wel (art. 126bb).
Kwalijker is dat de bescherming van geheimhouders bij onderzoek aan inbeslaggenomen voorwerpen en bij de netwerkzoeking, nu geregeld in art. 125l, lijkt te vervallen in het wetsvoorstel. Dit wordt nergens gemotiveerd en komt ons ook onbegrijpelijk voor. Het wordt veroorzaakt door het uiteentrekken van de bevoegdheden met betrekking tot geautomatiseerde gegevens in slechts twee trajecten: de doorzoeking en het vorderen van gegevens. Het vangnet dat nu – weliswaar onvolkomen – in de wet bestaat voor andere situaties van computeronderzoek valt weg, terwijl het eerder systematisch doorgevoerd zou moeten worden in plaats van afgeschaft.[50]
Overigens zijn ook de bepalingen die de verschillende wetsvoorstellen, Computercriminaliteit II[51] en vorderen gegevens, afstemmen voor het geval de ene wet eerder in werking treedt dan de andere, lacuneus. Vooral wanneer Computercriminaliteit II eerder in werking zou treden dan Vorderen gegevens, ontstaan problemen doordat niet meer bestaande bepalingen worden aangepast en andere bepalingen dubbel worden ingevoerd.[52]

[48] Anders dan u wellicht zou vermoeden, staan artikelen 126bb-dd *na* bijvoorbeeld art. 126na; een gealfabetiseerd artikelsgewijs register op Sv raakt het spoor volledig bijster in de almaar uitdijende 126-serie.

[49] Het wetsvoorstel Computercriminaliteit II paste de bewaringregeling – onzes inziens terecht – aan tot een regeling vergelijkbaar met de BOB-bepaling van art. 126cc. Het wetsvoorstel vorderen gegevens maakt dit echter ongedaan.

[50] Opmerkelijk genoeg worden aldus de bevoegdheidbeperkende bepalingen (vernietiging, notificatie, geheimhouders) beperkt tot de twee situaties van doorzoeking en gegevensvordering, terwijl tegelijkertijd een bevoegdheidscheppende bepaling is voorgesteld (ontoegankelijkmaking, zeg maar 'inbeslagneming' van gegevens ter onttrekking aan het verkeer) die in alle situaties van computeronderzoek mogelijk is. Zie het voorgestelde art. 125o Sv, *Kamerstukken II* 1998/99, 26 671, nrs. 1-2.

[51] *Kamerstukken II* 1998/99, 26 671, nrs. 1-2.

[52] Zie hierover de uitgebreide versie van dit artikel, te vinden op <http://www.gegeven.nl>.

L. Stevens, B.J. Koops & P. Wiemans (2004), 'Een strafvorderlijke gegevensvergaring nieuwe stijl'
Verschenen in: Nederlands Juristenblad 79 (32), p. 1680-1686.

5. Conclusie

Het bestaande wettelijke kader op grond waarvan politie en justitie beschikking kunnen krijgen over gegevens, biedt slechts beperkte mogelijkheden medewerking van houders van gegevens af te dwingen. In de praktijk wordt buiten dat kader al nauw samengewerkt door bedrijven en opsporingsinstanties op vrijwillige basis; dat is echter geen structurele oplossing en voor beide partijen weinig bevredigend. Het is daarom van groot belang de wet meer duidelijkheid schept over wat wel en wat niet kan binnen de gegevensvergaring. De Commissie-Mevis heeft daartoe een aanzet gegeven en doordacht werk geleverd met een hecht doortimmerd en overdacht voorstel. Daarbij moet wel worden aangetekend dat het commissievoorstel blijk geeft van een bepaalde visie op het strafrecht en de politieke balans, waarbij relatief veel aandacht is voor de behoeften van justitie om vrij eenvoudig gegevens te kunnen opvragen, en relatief minder aandacht voor de risico's die grootschalige gegevensbevraging bevat voor burgers, zoals verlies van hun goede naam.
De wetgever benadrukt echter binnen het kader van de veiligheidsmanie nog eens extra de opsporingsbelangen. In plaats van daar kritisch tegenover te staan, lijkt de Tweede Kamer vooralsnog alleen maar om nog meer verruiming te vragen. En de Raad van State heeft verzuimd om het wetsvoorstel te beschouwen met een constitutionele en wetssystematische blik. Nergens in de discussie over de voorstellen van de Commissie-Mevis of in de kamerstukken is ook maar enigszins aannemelijk gemaakt dat de nieuwe bevoegdheden in hun totaliteit ook werkelijk '*noodzakelijk* zijn in een democratische samenleving' in de zin van art. 8 van het EVRM.
Verder schort het voor de nietsvermoedende burger aan effectieve rechtsbescherming. Het adagium 'wie niets te verbergen heeft, heeft niets te vrezen' is te kortzichtig, omdat door de ruime opzet van de bevoegdheden ook veel onschuldige burgers door verzoeken van politie bij derden in een kwaad daglicht kunnen komen te staan. En de voorwaarden om zeer privacygevoelige gegevens op te vragen, zijn aan de lichte kant. Een mogelijke oplossing is om de bevoegdheden te beperken tot het opvragen van gegevens over verdachten.
Ook met de belangen van de bedrijven en instellingen die houder zijn van de gegevens wordt niet veel rekening gehouden. Dat geldt met name voor de kosten die het (mogelijk maken van) opvragen van gegevens met zich meebrengt, en die grotendeels voor rekening van de bedrijven komen. Een rechtvaardiger kostenverdeling lijkt ons hier op zijn plaats. Een kostenvergoeding voor elke bevraging van gegevens zou bovendien als gunstig effect hebben dat de natuurlijke informatiehonger van het opsporingsapparaat in toom wordt gehouden.
Volgende punten van kritiek liggen in het gebrek aan systematiek tussen de vele wetsvoorstellen op het gegevensgebied, en in het onder druk zetten van de systematiek van de strafvordering als geheel. Door het verlangen naar veiligheid en de snelheid waarmee de strafvordering daarop moet worden afgestemd, zijn in razend tempo verschillende trajecten uitgezet (computercriminaliteit II, vorderen gegevens telecommunicatie + financiële sector + algemeen, en er komt nog een wetsvoorstel aanpassing aan het Cybercrime-verdrag). Daarbij worden niet alleen details over het hoofd gezien, maar ook de reikwijdte van de combinatie van bevoegdheden, en er is zelfs sprake van aperte onjuistheden. Deze vergissingen (zoals het verdwijnen van de bescherming voor verdachte en verschoningsgerechtigden bij uitoefening van artikel 125k Sv en het lacuneuze afstemmingsrecht) moeten in elk geval worden rechtgezet.

Daarbij ware het verstandig om alle nog lopende trajecten op gegevensgebied ineen te schuiven in één overzichtelijk wetsvoorstel.
Wat betreft de strafvorderingssytematiek geldt dat gegevens ‘kleurloos’ worden benaderd als waren het voorwerpen. Daarmee wordt de enorme potentiële informatiewaarde van gegevens ontkend en lijkt het meewerken aan gegevensvergaring minder verstrekkend dan het werkelijk kan zijn. Het verzamelen van gegevens over boodschappen en aankopen, over locatie van mobieltjes en pin-transacties, over lidmaatschappen en surfgedrag op Internet, maar ook het opvragen van papieren dagboeken, agenda’s en persoonlijke aantekeningen – al die informatie maakt de verdachte en de burger transparanter dan ooit tevoren.
Het is dringend gewenst dat de wetgever, én de maatschappij (want ook de pers heeft vooral mediastilte laten vallen), zich bewust worden van de ingrijpendheid van de voorstellen. Een aanvaardbare wettelijke regeling kan alleen tot stand komen als het parlement kritisch tegenwicht biedt aan de neiging van de regering om opsporingsbelangen heilig te verklaren.